14 Communications Technology

14.1 Networks

network: Two or more computers or devices connected together so they can communicate and share data and resources.

Local Area Network (LAN):

- A LAN is a network that is limited to a small geographic area, such as a single building, a campus or a group of closely located buildings.
- It has high data transfer speeds of upto 1 GB per second.
- Data transmission errors are fewer because data is transferred over a short distance
- Normally connected using copper wire, fibre optics cables or radio waves.
- It can be kept more secure as a smaller number of devices need securing. The security is also the responsibility of network owners.
- There is usually private ownership as they are often owned, setup and maintained by single organization or individual such as a business, school or government institution. The organization has control over the LANs configuration and security.

Advantages:

- Enables efficient sharing of files, printers and applications
- Reduces costs by minimizing duplicate equipment
- Has high data transfer rates which allows fast communication and data exchange
- It has high scalability to accommodate the addition of new devices and network growth
- Facilitates centralized data storage and management on servers for better organization and security

Disadvantages:

- Initial installation and setup can be expensive

- Has a limited physical range / confined to smaller geographical area
- It relies on centralized hardware like servers and switches, making it prone to fail if the central components fail
- Easier to spread virus/more susceptible to security threats

Wide Area Network (WAN):

- A WAN is a type of computer network that spans a large geographical area, connecting multiple LANS and other network devices.
- It can be within a country or can spread across several countries.
- Internet is the largest WAN
- It is often restricted to lower transfer speeds normally less than 200 mb.
- It has greater chance of errors occurring as data is transferred over longer distance.
- Connections could include physical connections such as copper wire,etc and others like radio waves, microwaves, transmission towers and satellites.
- It is more susceptible to security issues as a large number of devices need securing. The organization will normally need to rely on the security measures of others for part of the network, so they will not be able to control security in these areas.
- Elements of the network are often owned by a third party, so they have to rely on the control and maintenance of others.

Advantages:

- It enables global connectivity and makes communication and resource sharing even easier.
- It is cost efficient since resources can be virtually shared
- Has high scalability, WAN can seamlessly grow with organizational expansion
- Enables remote access

Disadvantages:

- It has low latency, as data is transmitted over long distances
- Building and maintaining a WAN is expensive as a large geographical coverage needs to be covered and maintained.

- WANS are alot more complex to design, implement and manage compared to LANs as they require specialized knowledge and expertise.
- There is very limited control in WANS as a large number of devices/users need to be monitored and controlled and a lot of service is dependent on third parties/providers
- Due to a larger network setup, there is a higher risk of unauthorized access and breaches

Client-Server:

- A client server network is the one that contains two types of computers, a **client** and a **server**.
- The server(s) in a client- server network are a central point of control and provide a dedicated function for the network.
- All other computers in the network are all connected to the server to allow it to perform its dedicated function.
- Most client server networks operate using a request response method.
- A typical operation in this method is a client sends a request to a server to ask the server to perform a task and the server responds by performing the task.

Server Type	**Function**
File Server	Stores and manages data files. This saves the need for extensive storage space on client computers. They allow a user to use any client computer in the network and still be able to access their files and also any publicly shared files available. They also allow a central backup of all data to be made.
Web Server	Stores, processes and transmits web pages.
Mail Server	Sends and receives emails. It stores incoming emails for the user that can be downloaded when requested. It forwards outgoing messages to the correct destination. Most mail servers have security checking software that will scan emails for issues such as known viruses and malware. They can also be set to check for inappropriate content and spam.
Application Server	Installs and runs software applications. They provide a platform to run both desktop and web applications.
Print Server	Receives print jobs from client computers and sends them to the correct printer. This allows many client computers in a network to use the range of printers available. They can be set to print to a specific printer. They can also be set to find the next available printer or the closest printer to the client. If many jobs are sent to the print server at a time, it will queue the jobs until it can deliver them to a printer.

FTP Server	Manages the transfer of data that uses the file transfer protocol (FTP). It keeps a log of all activity involving FTP. Uses a lot in the transfer of files over the internet.
Proxy Server	Acts as an intermediary between clients and other servers by receiving client requests and forwarding them on to the relevant server. It provides an added level of security in a network, protecting clients directly accessing resources on another server. For this reason, it can also be set to act as a firewall.
Virtual Server	Shares the hardware of another server. Created using virtualization software on another server. Multiple virtual servers could be created on one physical server. A virtual server can be given the capabilities of any of the above physical servers. Businesses sometimes use third party virtual servers that will act as a web server, for the business to host its website. This allows the hosting company the ability to host several businesses websites on the hardware of a single physical server.

Advantages:

- Files can all be located in a single place and backed up on a regular basis. This means each user doesn't need to be responsible for this.
- Security for the network can be controlled from a central point, meaning each user doesn't need to be responsible for this.
- Levels of access can be applied o resources and data on servers, so only those that should have access will do so. This is very beneficial when some data ad resources have to be kept confidential.
- Updates for any software or network peripherals can be rolled out from a central location. Therefore, the business is not reliant on each user installing updates

Disadvantages:

- Can be very expensive to set up due to the need to buy expensive equipment, such as servers.
- Expensive to maintain as specialist knowledge is required to setup and maintain the servers.
- Failure of a server will mean that functionality is unavailable for all users. For example; no user can access their files if a file server fails.

Peer-To-Peer:

- A peer to peer network is decentralized network where each computer in it known as peers has equal status.
- Each computer shares its data and resources directly with each other without the need of a server.
- Similarly each peer stores its data on its own computer but may allow access to it to other peers or chose to keep it private.
- Each computer operates independently and there is no central dependency.
- It's easier to join/add more peers or remove them.
- Peers with varying processing powers can join and work on a collaborative task
- BItTorrent is an example of it.

Bit Torrent-

- A communication protocol often used in peer to peer file sharing.
- In it peers/node share the workload without the need for a central server
- They work as both client and server for other nodes/peers
- Several sources known as hosts are collated to create a swarm
- Each host will be given pieces of the file
- The BitTorrent protocol allows users to join the swarm and download the file from the available hosts
- For it a peer to peer/ Bit torrent client software is run on computer
- The protocol downloads the file in pieces, simultaneously from various hosts in the swarm
- The protocol can then rearrange the pieces to create a completed file
- Each piece of the file is protected to stop it from being modified by any users
- Each user trying to download the file is called a peer and each user providing the upload of the file is called is called a seed.
- Once a peer has piece of a file it can become a seed for the parts downloaded
- Tracker keeps record of all the peers and the parts of the file they have and can pause and restart at any time.
- Used to steam videos and transfer large files using minimum bandwidth
- Used by social media to distribute updates to servers

Advantages:

- Relatively cheap to setup as no need to buy expensive servers.
- Requires little technical knowledge to set up.
- Users are able to share data and resources.
- Often has less traffic than the alternative client server structure.
- Users have full control over the data stored on their computer.
- If a peer computer fails, this will only have a minor effect on the rest of the peer in the network. It will just mean that any data that the user had public will be temporarily unavailable.

Disadvantages:

- If a peer computer is being accessed by another peer computer, it can affect the performance of the computer and cause it to run slower.
- The data stored on each peer computer is not centrally backed up by the network. Therefore, if a peer loses the data, it is lost for everyone, unless they have a copy saved locally on their computer.
- The public files shared by a peer computer may be disorganized and difficult to navigate, because there is not central organization system in place.
- Each user in the network is responsible is responsible for the security of their peer computer. If users are not vigilant, and their computer gets a virus, this could be passed to other peer computers in the network.

Virtual Private Network (VPN):

- It is a secure technology that encrypts internet connections, providing privacy, anonymity and secure access to remote networks.
- It enables users to browse privately, access geographically restricted content and connect securely to corporate networks from anywhere.
- Open VPN Server -> creates a VPN -> software encrypts your data -> sends it to VPN server -> forwards it to destination // same happens in reverse
- If data is intercepted it will be useless since its encrypted and hacker wouldn't know the origin of data since it will show its send from the VPN server or its destination since it will show its sent to the VPN server.

Internet Protocol Security (IPSec):

- Network protocol that is designed to encrypt and authenticate data packets that are sent across the internet. It is also a part of tunneling process for a VPN.
- Encryption of keys at start of session/digital certificates are used for authentication/pre-shared keys (to be used) are negotiated/established at start of session
- All data (that is exchanged) during session is encrypted for different sessions
- Can support (both) pre-shared key/private and public key encryption of data so that the data is not understandable without the keys
- Works at Internet layer of protocol suites/stacks so encryption is at device level/supports VPNS

Tunneling:

- Data is broken into (small) packets/datagrams for transfer over IP network
- (IP) packets are encapsulated by Tunneling Protocol/L2TP inside (public) IP packets and sent out over public communication channels (to internet)
- Data is/may be encrypted using a secure shell (SSH)/IPSec protocol
- Packets are decapsulated and unencrypted at destination

Advantages:

- Data is encrypted before it is sent across the network.
- The identity of the sender is kept private from the destination and any hacker who intercepts a data package.
- The maintenance of the VPN server is not the responsibility of the user so they don't need to think about this.

Disadvantages:

- In some countries the use of a VPN is illegal or controversial, as some people can use them to create anonymity in certain criminal activity.
- The security of the data is reliant upon a third party and their ability to create effective software and maintenance of the VPN server.
- There is often a cost involved in purchasing a VPN. This could be a monthly subscription fee.

Mobile Networks:

- A mobile network also called a cellular network is a wireless WAN that uses radio waves to transmit and receive communications from portable devices such as smartphones.
- Mobile networks are broken down into small areas called cells which is the geographical area covered by a radio transmitter.
- At the heart of each cell is a radio base station that transmits and receives messages.
- The base stations connection to public telecommunication services allowing access to the internet.
- There have been several generation of mobile networks each providing faster access speeds and greater reliability. (1G, 2G, 3G, 4G, 5G)
- 1G: first generation of mobile networks uses analogue signals. It's also largely limited to voice and text message communications
- 2G: second gen which uses digital transmission, improving signal quality. It is able to connect with each other, allowing a phone to use other networks.
- 3G: it increased data transmission speeds upto to 2 Mbps, allowing mobile internet access, video transmission and online gaming.
- 4G: allows data transmission speeds of upto 1Gbps, allowing greater use of high quality video streaming facilities and advanced mobile services and online gaming.
- 5G: latest generation offering the fastest and most reliable connections available. It supports technologies like augmented reality, virtual reality and the internet of things (IoT). They have tested speeds upto 1.5 Gbps at present but could be even faster. Very large capacity for connection of devices/up to a million devices per km2. Very high bandwidth for transferring data between multiple devices. Very low latency in the connections for fast/instant responses. Seamless handover between base stations. Use

of ‘beam-forming’ techniques (by base stations) to direct signal/improve connections to (specific) devices.

Advantages:

- Mobile networks have enabled users to communicate with others and access the internet while on the move, often through the use of smartphones.
- Breaking the network down into cells allows for lower power radio transmitters to be used, bringing energy and cost savings.
- There are only so many radio frequencies that can be used for mobile communications. These frequencies can be split among neighboring cells and reused in more distant cells, thereby increasing the number of communications that can take place at the same time.
- Larger geographical areas can be covered than by using a single transmitter. Even high power transmitters are limited in range. By using several low power transmitters, a wider area can be covered.

Disadvantages:

- Quality of reception can vary and can be poor towards the edge of a cell, leading to interrupted or delayed transmissions.
- The use of frequency must be carefully planned to avoid interference between cells.
- The technology for 5G technology is limited at present at present and it could take a while and be costly to make the technology full usable.

14.2 Components in a network

Wireless / Network Interface Cards (WNIC and NIC):

- NIC assumes a vital role in the network communication by serving as an essential link between a device and the network infrastructure.
- Operating at the Data Link Layer, the NIC encapsulates data into frames, assigning source and destination MAC addresses for proper addressing within the local network.

- With a unique MAC address, each NIC identifies the device on the network.
- It establishes physical connectivity, whether through wired (Ethernet cable) or wireless (wifi) means.
- The NIC prepares data for transmission, converts it into frames, and transmits them onto the network
- Simultaneously it monitors the network for incoming frames, processes them and delivers the data to the devices operating system.
- NICs require driver software to communicate with the operating system, ensuring proper configuration.
- It collaborates with switches, routers and firewalls, to contribute to efficient, secure and seamless communication within the network infrastructure.
- An NIC can also be wireless WNIC providing the same function by using radio waves to transmit and receive data. It also works along a WAP (wireless access point)

Repeaters:

- A repeater serves as a signal booster in a network, extending the reach and coverage of the network by amplifying and retransmitting signals.
- It operates at the physical layer of the OSI model, receiving incoming signals, amplifying them to compensate any signal degradation over distances and regenerating the signals to remove any noise and retransmitting them back into the network.
- In modern networks with switches and routers, repeaters are less frequently used but they can still be employed to extend the reach of networks segments.
- In wireless networks, wireless repeaters are utilized to amplify and retransmit wifi signals, particularly in areas with no or weak signal coverage.
- Repeaters however due to address issues related to congestion or provide network segmentation and they may introduce latency (delay)

Hubs:

- A hub is used to connect a device to the network if there are multiple as they can’t be connected via Ethernet connection.
- If a data needs to be send to a device in the network, it will be first be sent to the hub which will forward the data to all connected devices.

- It will pass through all devices, the intended device will receive the data while others will simply ignore.
- A hub can be passive or active, a passive hub just sends data to all devices while an active hub will amplify and regenerate the signal used to send the data in order to make it stronger.
- This is due to the process of sending data to all devices being long and inefficient and hence deteriorating signals.
- A hub operates at the physical layer (layer 1) of the OSI model.

Switches:

- A switch is similar to hub as it connects multiple devices to a network and helps communicate data between a network.
- It operates at the data link layer (layer 2) of the OSI model.
- A switch examines each data packet it receives and forwards it to the intended devices only.
- It uses a MAC address source table of the connected devices.
- It looks at the mac address of the intended destination of the packet and compares it against it stored mac address table.
- It sends frames to the known addresses where its intended while all unrecognized data is sent to all addresses
- This reduces the possibility of data collision and increases network performance than a hub.

Wireless Access Points:

- A WAP allows a wireless device to connect to a wired network within a designated coverage area.
- It receives wireless data signals and then uses the wired network to transmit them to their destination often via a switch.
- Devices with wnic can connect to a network via WAP's SSID (service set identifier)
- It supports the connection of multiple devices to the same WAP, allowing them to connect to a network and effectively creating a wireless LAN.
- The connectable devices often have a limit.
- It extends the network so that computers don't need to be in a fixed place.

- The signals deteriorate with distance hence for large establishments multiple WAPs are used that may centrally managed by a wireless controller for coordinated performance.

Gateways:

- A gateway is a device or software that allows two or more different networks to connect to each other, enabling communication and data transfer.
- Router is a common gateway that connects two or more similar network
- Gateway is important in network connection as different network have different protocols and enables communication between them.

Bridges:

- A bridge is network component that joins different LANs together.
- It is responsible for segmenting and managing network traffic efficiently
- It divides a larger network into smaller segments, creating separate collision domains to minimize the chance of data collisions
- It operates at data link layer (layer 2) of the OSI model, filtering and forwarding traffic based on MAC addresses.
- It also maintains a MAC address table, containing the addresses of the connected devices of each network segment.
- It examines data packets as it receives and checks them against the MAC address source table, if they are intended for another network segment, it forwards it to that part of the LAN acting as a bridge
- If it happens to be in the same segment, then it simply ignores it and lets it travel to its destination like the switch

Routers:

- A router is a device that acts as gateway in connecting two or more similar networks.
- A router assigns each connected device with a unique IP address to identify its location in the network.
- *IP address can be IPv4 or Ipv6, Ipv4 is 32 bit long and the other is 128 bits long.*
- *IP addresses can also be static which means it stays the same if the device reconnects to a network or dynamic which changes if for every session.*
- *Most devices operate with a dynamic ip address and would need to request their internet provide for a static one.*
- A router can also be used to connect a LAN to a WAN.

- It forwards data packets to their intended destination between networks.
- It examines data packets and looks for their IP address of the destination to use it to send it to there
- Routers maintain a routing table which is stored in the router, which allows them to establish the most efficient route for the data packets to travel in.
- It makes use of routing protocols to help the select the route for the data to travel from one network to another.
- There are 3 main routing protocols, interior gateway protocol, exterior gateway protocol and border gateway protocols.
- Interior gateway protocols are used to specify how routers communicate with each other within a network such as LAN
- Exterior gateway protocols are used to specify how routers communicate with each other between different networks.
- Border gateway protocols are a specific kind of exterior gateway protocols hat manage the process of exchanging packets of data across the largest network, the internet.

Firewalls:

- A firewall is a network component that monitors and controls outgoing and incoming traffic in a network based on a set of defined protocols.
- It can block incoming traffic that doesn't meet the protocols, and maintain a blacklist of denied traffic/ sources
- Any data from them or to them is denied.
- It can also generate logs for monitoring and reporting purposes.
- Firewalls can also provide services like VPN
- Firewalls can be either hardware or software.

14.3 Network servers

File server:

Advantages:

- It provides a centralized file location for storage and organization of files ensuring easy access and management.
- It enhances data security by enforcing access controls and security measures, which safeguards data against unauthorized access and potential breaches
- Support regular backup and recovery option which contributes to data durability against accidental deletion or hardware failures
- It can support remote access, enabling users to connect and share or access files from outside the network, promoting flexibility and productivity for remote users.

Disadvantages:

- In case of file server downtime or malfunction, access to files will impossible unless a backup is available locally on device or on another file server
- Complete dependency for data storage on a file server can cause degrade the network performance as multiple request are made to access the data stored on a file server
- File server administration may become a complex task with setting user permissions, file access rights, backup configuration as the network grows more and more requiring skill staff.

Web server:

Advantages:

- Web servers simplify the deployment of web applications and content, making it easier for developers to publish updates and new features.
- Web servers can compress content before transmitting it to clients, reducing bandwidth usage and improving page load times for users.
- They generate logs that provide valuable insights into website traffic, user behavior, etc supporting analytics and performance optimization
- Web servers are scalable, capable of handling increased traffic and user demands by adding resources or optimizing configuration.

Disadvantages:

- Web server are susceptible to security vulnerabilities such as denial of service (ddos) attacks, data breaches and code injection, requiring constant monitoring and security measures to mitigate risks.
- Downtime or malfunctions can occur, disrupting access to website and online services for users
- It depends on stable and reliable internet connectivity, network issues or outages can impact the accessibility and responsiveness of websites and web application for users.

Mail server:

Advantages:

- Centralizes email management, enabling users to access emails from any device while ensuring synchronization and consistency across devices.
- Facilitates sending and receiving of attachments, enabling users to share files and documents securely within the email system
- Mail servers support the use of customized email domains, allowing organization and businesses to have professional and branded email addresses.
- Implements security features such as security and authentication, ensuring the confidentiality and integrity of email communications, protecting sensitive information from unauthorized access.

Disadvantages:

- During a downtime due to maintenance or technical issue, users may be unable to access their emails causing disruptions in communications.
- Its dependent on the stable internet connection, disruption in internet connectivity can impede access to emails and affect the overall reliability of the email system.
- Mail servers are susceptible to email spoofing, where malicious actors forge email headers to make messages appear as if they come from a trusted source, this can lead to phishing attacks and deception of users.

Applications Server:

Advantages:

- Application servers often act as middleware, providing additional functionalities like database connectivity and messaging services, this simplifies application development and integration processes
- Centralizes the management of web and desktop applications, allowing for efficient deployment, updates and maintenance in a unified manner.
- It supports scalability, enabling system to handle increased user loads and demand, crucial for applications that experience variable traffic levels.

Disadvantages:

- Running multiple applications on an application server can be resource intensive, requiring sufficient hardware resources to ensure optimal performance, this may lead to increased infrastructure costs.
- Server downtime can impact the accessibility of hosted applications
- May face compatibility issues with certain development frameworks, libraries or third party components

Print Server:

Advantages:

- It centralizes print management, allowing administrators to control and monitor print jobs, printer queues and configurations from a single location.
- It is resource efficient, as it optimizes resource usage by efficiently managing print queues, reducing the workload on individual computers and ensuring that printing jobs are processed in an organized and timely manner
- Enhances security by implementing access controls and permissions for print resources ensuring only authorized users can access specific printers and control their use

Disadvantages:

- If server experiences downtime or malfunctions, printing capabilities for all connected users may be disrupted.
- Print server may face compatibility issues with certain printer models, drivers or operating systems.

FTP Server:

Advantages:

- Enables efficient and fast transfer of files between computers over a network, making it effective for larger files or batches of files.
- It facilitates remote access to files, allowing users to upload or download data from anywhere with an internet connection; supporting collaboration and file sharing among geographically dispersed users.
- It supports authentication, requiring valid credentials to access files, ensuring secure and controlled access to the data.

Disadvantages:

- FTP doesn't inherently encrypt data during transfers, which poses a threat to sensitive information.

Proxy Server:

Advantages:

- Proxy servers enhance security by acting as intermediary between users and the internet. They can filter and block malicious content, control access to specific websites and provide anonymity by masking uses IP address
- It can cache frequently accessed content, reducing the need to fetch the same data repeatedly from the internet, saving bandwidth and allowing faster access to resources
- Proxy servers can distribute incoming network traffic across multiple servers, optimizing resource utilization and ensuring no single server is overloaded
- Allows content/ resources in a setting like office or school to be regulated and controlled, by restricting access, it filters inappropriate or non work related sites.

Disadvantages:

- It can introduce latency, causing delays in data transmission
- If the proxy server experiences downtime or malfunctions, it can disrupt internet access for users relying on it.
- Proxy servers often log user activities, and this data may raise privacy concerns. The storage and handling of logs must be managed carefully to comply with privacy regulations and prevent the potential misuse of user information.

Virtual Server:

Advantages:

- It helps in cost saving by reducing hardware requirements, lowering energy consumption and minimizing physical space needs
- Virtual servers provide an ideal environment for testing and development purposes, developers can launch code/application/load and test and experiment with various configurations without impacting the main network.
- Virtual servers allow for the consolidation of multiple virtual machines (VMs) on a single physical server. This optimizes resource utilization, reducing the need for multiple physical servers and improving overall efficiency.

Disadvantages:

- Virtual servers share physical resources, leading to potential resource contention. If not properly managed, competing virtual machines on the same host may impact each other's performance during periods of high demand.
- The stability and reliability of virtual servers depend on the host server's stability. If the host server experiences issues or failures, it can impact all the virtual machines hosted on that server, leading to downtime for multiple services.

Operations of servers in a server farm:

Servers collaborate to handle various tasks and ensure the efficient functioning of the overall infrastructure.

- They share the workload so that no single server is overloaded, this helps in making sure everything runs smoothly
- They have high availability so if one server experience issues or fails, traffic is redirected to available servers to minimize downtime and maintain uninterrupted services
- Dynamically allocates resources such as cpu, memory and storage based on the demands of the applications and services to optimize performance.
- Creates copies of data across multiple servers or locations to prevent data loss incase of hardware failure providing backup facility.

14.4 Cloud computing

Characteristics of cloud computing:

- Cloud computing is a technology that provides on demand access to a shared pool of computing resources over the internet.
- This includes storing data on remote server over the internet
- These servers are maintained by third party companies.
- The access is often via use of web browser
- It can involve the use of VPN for secure connection.
- The devices and data/file servers are location independent/can be accessed from any location with internet access
- The resources are shared between client company and provider
- It can be dynamically changed by provider as and when required without client intervention.
- Various service models exist, e.g providing the infrastructure/providing the software only/ providing the 'computing platform'/ development environment.
- Cloud computing can be divided into 3 main categories:
- **Infrastructure as a service (IaaS):** in this model of cloud computing the host provider hosts some of the network resources that are used by businesses, such as servers. Businesses can gain access to these resources using the internet.
- **Platform as a service (PaaS):** In this model of cloud computing the host provider hosts platform resources that can be used to build software applications. Users can gain access to these resources using the internet.
- **Software as a service (SaaS):** In this model of cloud computing, the host provider hosts software applications and makes them available to users using the internet.

- Cloud computing resources can be quickly scaled up or down to accommodate changes in demand. This elasticity ensures that computing resources are readily available for sharing, adapting to varying workloads.

Uses of cloud computing:

- It is used for storage and backup
- It offers web based email services, custom mail server & access of emails from anywhere anytime with internet
- IaaS, business rent virtualized computing resources, including servers, storage and network, eliminating hardware requirement
- PaaS, Offers online platforms to build and run software without having to worry about the technical stuff
- SaaS, delivers software applications over the internet, eliminating the need for users to install, maintain and update software locally.
- Allows connecting and managing smart devices like thermostats and cameras online.

Advantages of Cloud Computing:

- Individuals and organization don't need to purchase additional hardware to store data and software.
- Individuals and organization don't need to host their own development platforms to develop applications software.
- Organizations don't need to employ technical staff to maintain the hardware used to store data and software that is provided by the cloud provider.
- Individuals and organizations don't need to worry about creating a backup of their data, because this is automatically carried out by the cloud provider.
- Individuals and organizations can access their data and software applications from anywhere in the world as long as they have an internet connection.
- Organizations can quickly boost the performance of their network by employing more resources from the cloud, If an organization is expecting more data traffic to their server, for example, they are having a sale of their products accessed by their website, they could increase the capacity of the webserver to allow it handle the temporary

increase in traffic. They could then reduce it again after the sale, to save costs.

Disadvantages of Cloud Computing:

- Individuals and organizations are reliant on a third party to keep their data secure and they have little control over the security measures that are put in place by the cloud provider.
- If the resources provided by the cloud provider fail, for example, a server fails, then the data or software stored on that server will become unavailable.
- Cloud computing resources can only be accessed using an internet connection, so if a internet connection can't be found, the resources can't be accessed.
- Owner of data may have no idea where the data is stored so may not be aware that is being stored in another country.

14.5 Data transmission across networks

Bandwidth:

- Bandwidth is the range of frequencies available for a communication method which determines the transmission rate.
- It is the maximum potential amount of data that can be transferred across a network within a given time, which is usually one second.
- The more bandwidth a connection has, the more data it can transfer at a single time.
- It is often measured in Hertz (Hz)
- It's important to note that bandwidth is not the same as speed, it represents the potential capacity of data transfer rate which speed is the actual data transfer rate experienced by users that is influenced by various factors like latency and efficiency of the device

Bit Rate:

- Bit rate is the rate at which bits can be transferred in a data transmission in a given period of time.
- The bit rate of a transfer will not exceed the bandwidth, because the bandwidth will be the maximum possible bit rate

- It's usually expressed in bits per second (bps) or its multiples such as kilobits per seconds (Kbps)

Real Time and On Demand Media Streams:

- There are two different types of data streaming- real time and on demand streaming
- In real time data streaming, the data is streamed as soon as it is recorded by the camera or any other recording device that may be used
- In on demand streaming, data is pre-recorded and streamed to the users device whenever they request the recording
- When a file is streamed, it removes the need to download and store the whole file before it is viewed or listened to.
- Data is streamed as a series of bits to the receiving device
- The receiving device will have a temporary storage area called a buffer
- Data will be stored in the buffer, as it is downloaded, before it is needed as the video is viewed, or the song is played.
- Data is removed from the buffer to be played and simultaneously added to be ready to play when required
- The bandwidth available will limit the quality of sound or video file that can be streamed
- If user has a connection that has bandwidth of 2 mbps, it is highly unlikely they will be able to stream a 4k movie from an online streaming service
- The required to produce each frame in the video would be too much to be transmitted using the bandwidth available.

Impact of Bit Rate and Bandwidth on the streaming of audio and video data:

- Bit rate represents the amount of information/data that is stored per unit time in the streamed/recorded video
- Bandwidth of available connections determine bit rate that can be used for the video
- If transmission medium does not have sufficient bandwidth to carry the required it rate the video will stall/be jerky/impose constant buffering
- …. And reduce the viewer's quality of experience of the video
- Video can be sampled at different bit rates/compressed to different bit rates
- Low bit rates produce video that lacks detail/is pixelated/shows motion in jerky steps

- The more bits that are used the higher the quality of the video e.g.
- … 16kbit/s is suitable only for video phone applications as detail is lacking/ any significant movement pixelates the image
- …2.5 Mbit/s is suitable for low quality internet streaming
- …9.6 Mbit/s is DVD quality
- …8 to 15 Mbit/s is HD quality
- ….40 Mbit/s will allow 1080p/Blue-ray disc quality for the videos

14.6 Routing data in networks

Structure of a data packet

- A data packet is normally the smallest unit of data that is sent across a network and it contains several elements.
- These elements can depend on the network used to send the packet.
- For example, if a packet is sent using the internet, it will contain more elements to allow to it to be directed to the right place.
- The normal elements of a packet of data are the **header**, the **payload** and the **trailer**
- The **header** could include:
    - The IP address of the sender. This is called the source of IP address
    - The IP address of the receiving device. This is called the destination IP address
    - The sequence number of the packet. This is so the receiving device can reorder the packets to obtain the original data.
    - The MAC (media access control) address of the send and the receiver. If the packet passes through a router, these will be removed as they are only used bu a switch
    - Any protocols used
- The **payload** will include:
    - The actual data from the file that is being transmitted
- The **trailer** could include:
    - A flag that tells a device it has reached the end of the packet
    - Any error checking methods that are used
- The data sent in the header and trailer are all designed to make sure that payload data arrives at its intended destination without any errors.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go but it is divided into smaller units which are sent individually.
- These small units are called data packets and they are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its header such as source address, destination address and sequence number
- Packets will travel across the network, moving from router to router, taking the shortest path possible set by the router
- Each packets journey time can hence differ
- All the packets are reassembled at the receiving end in correct order
- If any packet is missing or corrupt, then the message will be sent to resend the message
- If the correct order of the packets is reached then the acknowledgment message will be sent.

There are two main method of transmission in packet switching, **connection oriented** (also known as virtual circuit switching) and **connectionless** (also known as datagram switching).

Connection Oriented:

- In a connection oriented switching, a session is created before any data is transferred.
- This becomes a fixed channel for the data to travel
- The first packet sent includes a request for an acknowledgment.
- If the acknowledgement is received, the sender transmits further packets.
- If no acknowledgement is received, the sender tries again with the first packet
- Frame relay and transmission control (TCP) are two types of connected oriented packet switching.

Method	Function
Frame Relay	In frame relay, data is separated into units called frames. Any methods of error correction that are used are carried out by the devices at the end points of transmission, which is one advantage of frame relay, as it helps speed up transmission.

	If an error is detected in a frame, that frame is dropped. The devices at the endpoints will then detect the dropped frames and retransmit them. This makes frame rate most suitable for sending data where the error rate is likely to be low. There are two main methods of connection in frame relay. The first is permanent virtual circuits (PVC), which are connections intended to exist for long periods of time, even if data is not currently being exchanged. The second is switched virtual circuits (SVC), which are temporary connections designed to exist for a single session.
TCP	In this protocol, a connection is created and maintained until the application software at each endpoint have finished exchanging data. It determines how the data is broken down into packets, which it gives to and receives from the network layer in TCP/IP model. It is responsible for providing error free data transmission and managing the flow of the data.

Connectionless:

- In connectionless switching, there isn't any prior arrangement setup between devices to transmit the data
- The packets are dispatched with no knowledge whether or not the receiver is ready to accept the packet
- It also has no way to find out if the transmission has succeeded
- Ethernet, internet protocol (IP) and user datagram protocol (UDP) are types of connectionless packet switching.

Method	**Function**
Ethernet	This is a traditional protocol used to connect devices, using a wired connection, to form a network. It makes sure that network devices format and transmit data in a way that other devices on the network will understand. Most networks that are setup within a home or school are likely to use 25thernet.
IP	This is the protocol that is used when data is sent across the internet. It is the protocol that is responsible for delivering the packets of data to the receiving device.
UDP	This is an alternative protocol to the TCP. There are two main differences between this

	protocol and the TCP. The first is that this protocol sends the data in units called data grams. The second difference is that this protocol does not control the flow of data or carry out error checking. For this reason, the exchanging of data using UDP is often faster than using TCP

Circuit Switching

- Circuit switching is a technique that establishes a dedicated path between sender and receiver
- In the circuit switching technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated
- Circuit switching in a network operates in a similar way as the telephone works
- A complete end to end path must exist before the communication takes place
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgement, dedicated path transfers the data.
- Circuit switching is used in public telephone network, it is used for voice transmission
- Fixed data can be transferred at a time in circuit switching.
- While one computer is sending data using a certain path, no other computer in the network can use the same path.

Circuit Switching Steps

- The sender provides the identity of the intended receive
- The system checks whether the receiver is ready to accept the data
- If the receiver is available, a sequence of links is established across the network.
- The data is transferred
- The links are removed

Message Switching

- Message switching is switching technique in which a message is transferred as a complete unit and route through intermediate nodes at which it is stored and forwarded.
- In message switching technique, there is no establishment of a dedicated path between the sender and receiver
- The destination address is appended to the message, message switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forwards it to the next node. This type of network is known as store and forward network.
- Message switching treats each message as an independent entity.

IP Addressing:

- IP address are used to identify a location of the device in a network / used to uniquely identify a device on the internet
- IP address can be Ipv4 or Ipv6, Ipv4 is 32 bit long and the other is 128 bits long.
- IP addresses can also be static which means it stays the same if the device reconnects to a network or dynamic which changes if for every session.
- Most devices operate with a dynamic ip address and would need to request their internet provide for a static one.

MAC Addressing:

- MAC address is used to identify a device on a network through the means of an NIC card
- It is positioned at data link layer(layer 2) of the OSI model, they are important for local network communication.
- It allows device identification within the same network segment, enabling routers to forward data appropriately
- The address resolution protocol (ARP) relies on MAC addresses to map IP address within the local network
- The uniqueness of MAC address ensures no duplication of it and prevents address conflicts. It’s made up of manufactures ID number and serial number of the device

- In wireless networks, mac address assist in access control
- Mac address also contributes to filtering, allowing administrators to control network based on device addresses.

14.7 Network protocols

Protocol:

- A protocol refers to a set of rules used for transmission and receipt of data between devices on a network
- Protocols define the format, timing, sequences and error checking of data exchanged over a network, ensuring consistent and standardized communication.
- They are essential for devices from different manufacturers to interact seamlessly.

Transmission Control Protocol (TCP)

- Sends messages/data (in datagrams) using IP
- Provides checksum/port numbers for source/destination (of datagram)
- Used in connection-oriented communication/point to point
- Reporting to sender of lost/damaged packets
- Establishes how data is transferred over network
- Manages flow control
- Handshaking is carried to establish connection
- Used when delivery of datagrams is important
- Error checking

Internet Protocol (IP)

- Allows communication of different devices over the internet
- Provides unique addresses for each device o uniquely identify them
- Ensures correct routing of packets of data over the internet

- Takes a packet from transport layer and adds its own header which includes IP address of recipient and sender
- Encapsulate data into datagram
- Passes datagram to the link layer for transmission on the LAN.

Internet Control Message Protocol (ICMP)

- An error reporting protocol that is used to generate error messages, to transmit it to the sender, when network problems cause delivery problems with data packets

Address Resolution Protocol (ARP)

- The protocol responsible for translation of an IP address into a MAC address for a device.
- It is necessary for use between the network layer and the data link layer of the OSI model

Inverse Address Resolution Protocol (IARP)

- This protocol performs the opposite role to the ARP. It translates a MACC address into an IP address.

Dynamic Host Configuration Protocol (DHCP)

- It is a network management protocol
- Automatically assigns IP addresses to devices on a network
- It automatically assigns gateway address
- It automatically assigns a subnet mask
- Creates a database and manages the assignment of he addresses to avoid addressing conflicts

User Datagram Protocol (UDP)

- Sends messages/data (in datagrams) using IP
- Provides checksum/port numbers for source/destination (of datagram)
- Used in connectionless communication
- No reporting to sender of lost/damaged packets
- Used when delivery of datagrams is not important to the service
- Avoids overheads of processing of error checking/delivery status
- No handshaking
- No guarantee of delivery/order of datagrams
- No error checking

Hypertext Transfer Protocol (HTTP and HTTPS)

- HTTP is the protocol used for transferring content of web pages across the internet, from a web server to a browser
- HTTPS is extension of HTTPS that provides secure communications
- Encrypts using TLS/SSL
- Protects/ensures the integrity of data sent to/from website over internet/through the networks
- Operates at application layer to encrypt/decrypt using TLS
- Authenticates website using a (public key) certificate
- Controls access by restricting access to the site to authorized users
- Protects the privacy of data sent to/from website over internet/through the networks
- Protects against man in the middle attacks/eavesdropping on the data
- Protects against alteration/modification of websites
- Protects against insertion of malware, malicious code into website code

File Transfer Protocol (FTP)

- It is responsible for the transfer of files between a client and a server in network

Tunneling Protocol

- A communication protocol used for secure transmission of data over networks
- Makes use of encapsulation which allows private data packets to be sent across public network by making them look like public data packets
- Data is/may be encrypted using SSH/IPsec protocol
- An important protocol used in VPNs to allow data to be kept private
- Used to circumvent firewall rules to allow access to internal network by data carried in packets
- Allows the use of foreign protocols on networks that don't support that protocol, eg use of IPv6 on IPv4 networks

Simple Mail Transfer Protocol (SMTP)

- It is used send email from a computer to a mail server and between different mail servers

Post Office Protocols

- It is used to retrieve emails from a mail server.
- When the user checks their mailbox the email is sent from the server to their device.
- The protocol deletes the email from the server
- Eg; POP3

Internet Message Access Protocol (IMAP)

- The protocol used to retrieve email from a mail server
- It has one main difference from POP and that is that the email isn't deleted from the server by the protocol
- Only deleted when the user chooses to delete it

Telnet

- It allows a user to connect remotely to another computer using the internet
- Data is sent in plain text
- Connections are not authorized
- It lacks encryption, posing security risks and has been replaced by alternatives like SSH

Secure Shell (SSH)

- Provides a secure way to access computer over an unsecure network
- Encrypts data (is ended to end to end between application/software/apps)
- Uses client server model
- Connects application/program/app/terminal with a remote server
- Works at application layer of TCP/IP/OSI protocol suites
- (Uses authentication with) automatically created (private/public) keys (to provide encryption of data)
- (Provides encryption) so that observer/interceptor can't understand/not make sense of the data

TLS/SSL

- SSL is a network protocol that is designed to ensure connections made between web clients, such as user devices and web/mail servers are secure
- It uses both public and private keys to encrypt data that is transmitted over the secure connection
- TLS is an updated version of SSL
- It uses updated and more secure encryption algorithms

14.8 The management of network traffic

Routing

- Routing is the process of creating the route or the data packets and it occurs in the network layer of OSI model.
- It is used in routers/routing devices to determine the next node/router/device/hop to send data packet/datagram/frame
- Algorithms create a 'forwarding table'/routing table for use when choosing next hop/preferred route
- Routing tables are stored in nonvolatile memory of router hardware
- There are two types of routing; static routing and dynamic routing
- They both provide default route for packet if no route can be determined.

Static Routing Tables

- Routes are entered into a database/routes are decided/controlled by network administrator
- Route entries are fixed/don't change/are not configured automatically
- Defines fixed routes for packets to take from the router
- Used by a routing algorithm to create a 'forwarding table' for use when choosing next hop/preferred route
- Defines route of last resort/exit point from router/route to send packet if no destination is known
- Provides fail safe if dynamic routing does not provide a route
- Can be used to transfer routing information from one route to another/one routing protocol to another

Dynamic Routing Tables

- Routing protocols create a table of routing information from real time logical network layout/changes/issues/problems
- Created automatically by algorithms/not created by network administrator
- Use a number of different protocols/methods to determine best route/next router to use
- Routing information can be automatically shared with other routers (using same protocol)
- Routing information can be automatically shared with other routers to discover data about remote networks/changes in networks

- Can be used to limit the number of hops that packet can take to its destination
- Routes have a time to live after which the database/table will be updated
- Packets can be forwarded via different routes depending on network conditions
- Packets can be routed around network issues/damage/loss of a node/router
- Allow as many routes as possible to be kept open.

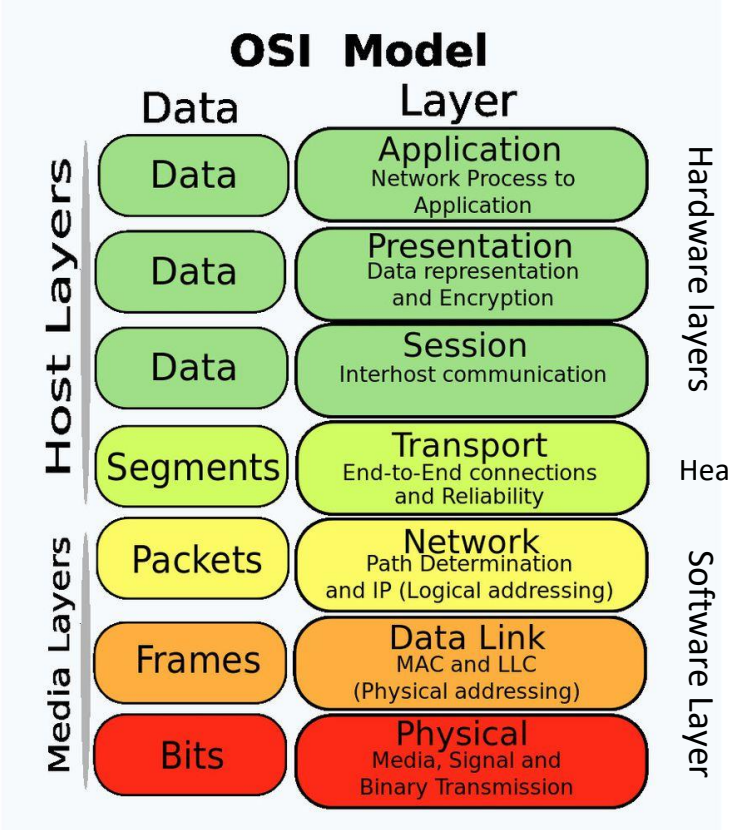
Function of Routing Protocols

- Routers use routing protocols to specify how they communicate with each other
- Routing protocols help select the route that data travels from one device in a network to another
- There are 3 main routing protocols, interior gateway protocol, exterior gateway protocol and border gateway protocols.
- **Interior gateway protocols** are used to specify how routers communicate with each other within a network such as LAN
- **Exterior gateway protocols** are used to specify how routers communicate with each other between different networks.
- **Border gateway protocols** are a specific kind of exterior gateway protocols that manage the process of exchanging packets of data across the largest network, the internet.

Open Systems Interconnection Model (OSI Model)

Layer	Function
Application	This is type top layer of the model that directly interacts with data from the user. Software applications such as web applications and email clients rely on the applications layer to communicate. However, user applications such as word processing packages are not included in this function The applications layer is responsible for managing the protocols that allow meaningful data to be presented to the user. It manages protocols such as hypertext transfer protocol (HTTP) and simple mail transfer protocol (SMTP)
Presentation	The primary function of the presentation layer is to prepare data ready for use in the applications layer. This could involve the translation, encryption and compression of data/ It makes sure that the data is translated into a form that will be understood by the receiving device. If the devices are communication over a secure connection, the data will be encrypted. it

	will also decrypt any data that is received. It will also compress and decompress any data that is required to increase the speed of transmission
Session	This layer is responsible for opening and closing communication links between devices. The time that passes between a communication link being opened and closed again is called a session. This layer makes sure that the session is open for long enough to allow all the data to be transmitted and then closes it immediately, as soon as transmission is completed
Transport	This layer is responsible for breaking down the data from the session layer into segments. These segments are then given to the network layer; it is also responsible for reassembling the segments at the receiving device. This layer is also responsible for flow control (the best speed for transmission) and error checking, it checks that all the data has been received and will request a retransmission if it is not complete
Network	The network layer breaks down the segments from the transport layer into smaller units known as packets. It's also responsible for reassembling the packets after transmission. This layer is also responsible for routing, which is the process of finding the best path across the network, the network layer performs these tasks when data is transmitted from network to network, a router is one of the key network components in this layer
Data link	This layer performs a very similar role to the network layer but rather than transmitting data from network to network, it is responsible for transmitting data from node to node within a network, it takes the packets created at the network layer and converts them into frames. A switch is one of the key components in this layer
Physical	This layer involves the physical equipment that is used to transmit the data, such as the cables. In this layer, data is broken down into bits to be transmitted as binary. This layer is also responsible for reassembling the bits into frames, after transmission



Heart of OSI

TCP/IP Model

Layer	**Function**
Application Layer	This layer condenses the role of the application, presentation and session layers from the OSI model. It uses several protocols to provide a standardised exchange of data. The protocols it uses include HTTP, SMTP, POP and FTP
Transport Layer	This layer is comparable to the transport layer in the OSI model. It is responsible for maintaining end to end communications between devices. There are two main protocols that at this level. The first is the TCP and the second is UDP
Network layer	This layer can also be known as internet layer and it is comparable to network layer in OSI model. It breaks data down into packets and transmits it network to network. There are two main protocols that are used at this level. The first is the IP and the second is ICMP
Link layer	This layer can also be known as the physical layer and it condenses the role of the data link layer and physical layer from the OSI model. A protocol used at this level is the address resolution protocol (ARP)

Similarities between OSI and TCP/IP Models

- Uses a logical framework for defining/implementing network standards
- Uses layered structure/architecture to describe/standardize the functions of protocols
- Each layer only defines/describes a specific/set of function/only that function
- Complex functionality is divided into simpler sections for easier understanding of network functionality
- Existing standards are referenced by layers/functions of layers
- Define standards/functionalities that allow manufacturer to create/produce devices/components that work with other manufacturers products

Differences between OSI and TCP/IP Models

- OSI model has seven layers whereas TCP/IP model has four/five layers/more layer in OSI than in TCP/IP model
- OSI functionality at application level has three separate layers to cover/include TCP/IPs one/single application layer application layer/application layer in TCP/IP is application + presentation + session layer of the OSI model
- OSI has separate physical and data link layers whereas TCP/IP originally combined these into one layer/Link layer
- OSI network layer provides for both connection oriented and connectionless links whereas TCP/IP network layer provides only for connectionless
- OSI Transport layer provides only connection oriented link where TCP/IP Transport layers provides for both connection oriented and connectionless links
- OSI Transport layer provides for a guarantee of the delivery of packets whereas TCP/IP Transport layer doesn't

14.9 Data transmission methods

Fibre Optic

- Fibre optic is a type of cable that is made up of lots of very fine threads of glass
- Electric signals converted to light for transmission / converted back to electrical signals after transmission

- LED / laser (at node) sends / transmits a light beam / electromagnetic wave along the fibre
- Data is modulated onto a carrier wave
- Optical fibre connects the nodes devices
- ADC / DAC are used to modulate / demodulate the data onto / off carrier wave
- Laser is used where longer distances are to be covered
- Led is used where shorter distances are to be covered as it is cheaper than laser
- Lasers produce coherent light which can allow greater bandwidth
- Receiver is photo detector to convert light into electricity
- Uses indium gallium arsenide in photo detector

Application:

- They are used in modern internet connection and in high performance networks where large amounts of data are transmitted
- They are also used in applications which requires long distance connectivity such as telephone signals

Advantages:

- Has the highest level of bandwidth available of the three cables
- Can carry signals for a much longer distance as there is less interference
- Difficult to hack so more secure
- Consumes less power
- Lighter in weight
- Requires less signal boosting

Disadvantages:

- Has the highest cost for manufacture and purchase
- Doesn’t not carry power only data
- Difficult to terminate
- Can be difficult to install due to how fragile the glass tubes can be

Copper Cables (coaxial)

- Coaxial is a type of copper cable that has a central wire surrounded by an insulating layer
- Coaxial cables also are used to carry radio frequency signals

Application:

- Used in applications such as TV and cable tv connections
- They are also used in some internet connections

Advantages:

- Low cost of manufacture and purchase
- Lower error rate because the central wire is within a faraday shield(a special shield used to block magnetic interference).
- More flexible
- Easier to terminate

Disadvantages:

- Has the lowest level of bandwidth of the three cable types
- Need repeaters
- The way in which a coaxial cable is insulated can make it difficult to install and maintain

Copper Cables (twisted)

- Twisted pair is a type of copper cable that has two separate insulated wires that are twisted around each other,
- These cables are then covered by an outer layer that acts like a jacket
- Twisted pair cables transmit electric current

Application:

- They are used for telephone communications
- They are used as part of an ethernet network

Advantages:

- Crosstalk (a signal transmitted from one channel to another) is minimized
- Is the lowest cost to manufacture and purchase
- Has a higher level of bandwidth than coaxial
- More flexible
- Easier to terminate

Disadvantages:

- Can be susceptible to electromagnetic interference
- Need repeaters
- Has the shortest distance that a signal can be carried before it will begin to deteriorate

Lasers

- Lasers can be used as a communication system.
- Unlike the tiny LEDs used in fibre optic communication, this method uses high power laser beams to transmit light signals
- It is sometimes called a free space laser system because the beams travel directly through the air
- For example, setting up a high bandwidth data link between two line of sight buildings can make use of a free space laser system
- There are commercial systems available that offer gigabit Ethernet connection speed upto 3 kilometer

Application:

- Between spacecraft (in orbit through vacuum)

- To connect sites across roads/other barriers not owned by sender/receiver
- Provide (temporary) network connection in e.g disaster areas where cabling is not possible

Advantages:

- They send more data in a single downlink than comparable radio systems
- They are ideal for space missions because they need less volume, weight and power
- They offer very high speed broadband

Disadvantages:

- Short range only in atmosphere due to dispersion of (light) beam by particles in atmosphere
- Accurate aiming of (light) beam is more/may be more difficult
- Difficult in connection is increased if sender/receiver are moving
- Blocked by objects/weather I path of (light) beam/line of sight

14.10 Wireless technology

Wi-Fi

- Uses radio signals and is the most commonly used wireless communication method
- Each device that wants to make a wireless connection will broadcast wants to make a wireless connection will broadcast a radio signal
- A router or WAP will receive these wireless signals and process them
- The router or WAP will also broadcast radio signals that will be received and processed by each device when it is receiving data that has been transmitted
- Wi-Fi currently transmits data at frequencies of 2.4 GHz and 5GHz
- These frequencies are much higher than those used by mobile networks
- These are high frequencies used to send larger amounts of data
- The current limit for Wi-Fi data transmission is approximately 450 Mbps

Advantages:

- Several wireless capable devices can connect to a single router or WAP
- The high level of frequency used means that large amounts of data can be transmitted at a time
- More recent wifi standards are backward compatible with previous ones
- Has quite a large range of approximately 100m
- It doesn't require a line of sight, so it can work through obstacles

Disadvantages:

- The speed at which data can be transferred decreases as more devices connect to a wireless network
- Less secure than a wired connection
- Radio signal can be subject to interference

Bluetooth

- Bluetooth also uses radio signals to create a wireless connection between two to upto 8 devices
- It uses the radio frequency 2.45 Ghz
- It has a lower bandwidth
- Bluetooth doesn't usually use a central access point
- Bluetooth is symmetrical
- To establish a connection, devices need to be within 10m of each other and there is currently a limit of eight devices that can be connected at any given time using Bluetooth
- These two devices requesting a wireless connection using Bluetooth must have matching profiles
- This is to stop pointless Bluetooth connections being made.

Connection Process:

- Turn on/open Bluetooth on both devices
- Ensure that the devices are in range/can detect/find each other
- Set one device to search for available devices
- Device is found/selected/responds/discoverable
- Device requires a passcode/user response by e.g. pressing a button/key/passcode entered/default passcode sent
- Passcode checked (by both devices)/connection/passcode confirmed on other device
- Devices are paired
- Frequencies/channels to use are decided.

Advantages:

- It requires a low level of consumption
- It doesn't require a line of sight, so it can work through obstacles
- Can be made more secure by requiring a pin code for connection
- There will be less interference as other wireless connections transmit on different frequencies

Disadvantages:

- As a limit of 10m for a connection
- A limit of eight devices can be connected at a time
- Has a lower level of bandwidth available than wifi

Infrared

- Infrared connections used infrared radiation as their method of connection
- Two different types of infrared connection can be made; line of sight mode and scatter mode
- In line of sight mode, there must be a direct line of sight between the sending device and the receiving device
- There should be no obstacles in the way
- In scatter mode; a device broadcasts infrared into a certain area and any device may receive it directly or through reflection of an obstacle

- The sending device will need the ability to produce an infrared signal and the receiving device needs an infrared sensor to capture the infrared signal
- Infrared lasers can also be used to transmit data from one device to another in a network
- The infrared laser beam needs to have a direct line of sight in order to be able to connect the devices
- Laser data transmission works in a similar way to fibre optic, in that it uses the properties of light transmit the data
- However laser transmission relies on data travelling through free space

Advantages:

- It is the most secure form of connection
- Low cost to manufacture and purchase
- It requires low level of power consumption
- It doesn't get any interference from radio frequency
-

Disadvantages:

- Can't be transmitted through obstacles
- If it uses line of sight mode, there must be a direct line of sight between the two devices
- It can only be used to connect two devices
- It has a short range with a limit of approximately 1m.
- May be subject to interference from bright sources

Microwave

- Uses wireless technology/beam of radio/electromagnetic waves
- Uses line of sight between antennae/send and receive antennae
- Uses frequencies in the range 300 MHz to 300 GHz
- Uses parabolic dishes with horn antennae to provide 'spot' beams

- Uses multiple antennae to send/receive signals
- Data is modulated onto carrier wave using orthogonal frequency division multiplexing/ orthogonal frequency division multiple access/ using a range of frequencies
- Pulsed transmission of waves/polarized with matching of antennas at both ends in horizontal/vertical form

Uses:

- Used by mobile systems in 3G/G/5G communications
- Used by Wi-Fi systems to link devices into a LAN
- Used for communications between base stations and satellites/uplink and downlinks with satellites
- Used in television/radio industry to transmit programmes from outside studio to studio/outside broadcasts (instead of expensive satellite links)
- Used to carry cellular/mobile phone systems data between masts/stations/to provide backbone carrier system
- Used for short-range indoor communications between devices
- Use to link remote/regional telephone exchange to main exchanges without the use of copper/optical fibre cabling.

Advantages:

- Small/directional antennas point directly at each other so can use same frequencies as neighboring transmission without interference/make economical use of radio spectrum
- Directional antenna provide increased performance with low power requirements
- Narrow microwave beams don't interfere with other equipment
- Small antennae/devices can be used so operations can be mobile eg TV sporting transmission/can be setup quickly to cover unfolding events/can be used in portable radio systems
- Have large bandwidth so can carry greater amount of data compared to any other medium

Disadvantages:

- High tall antennae may be environmentally problematic/difficult to install in some areas

- Line of sight required so antenna cant be over horizon/ limited to 50 to 08km apart
- ….so any obstacle will interfere with transmission
- …so can be interfered with/intercept
- Unable to penetrate obstacles/building/hills so positioning of antennas may be intrusive/unsightly
- Weather environment conditions can adversely affect the transmission
- 'Rain fade' due to absorption of microwaves by water can degrade the signals
- High pollen counts/dust/smoke can degrade signals due to scattering of signals by particles
- Solar events may affect transmissions/signals so interfere with communications
- Most of signal passes through antennae so transmissions can be intercepted behind official antenna/in space by satellite so security can be compromised.

Radio Waves

Advantages:

Disadvantages:

Security:

- there can be security issues associated with the use of wireless data transmission
- this is because wireless connections don't have same level of protection as a wired connection
- wired networks are normally limited to the confines of a building or single site and there are often locks and other security methods in place to stop an unauthorized person entering that area and gaining access to that network
- there are two main protocols that are designed to improve the level of security of a wireless network, wired equivalent privacy (WEP) and wi-fi protected access (WPA)
- WEP: This protocol is designed to provide a wireless network with a compatible level of security to a wired LAN. It does this by encrypting data transmissions sent using a wireless connection
- WPA: this is a standard required of devices equipped with a wireless internet connection. It is designed to provide a more sophisticated encryption than WEP.

Limited content so do comparison questions from pastpapers n memorize them

14.11 Mobile communication systems

Structure of a cellular network

- Base stations (in a cell/cellular subsystem) for (wireless) connection to end user
- Core/central switched network for handling voice calls/text messages
- Packet switched network for handling (mobile) data/internet traffic
- Public switched telecommunications/telephone network for connection into the global telephone networks

Explain how cellular networks allow large numbers of mobile (cell) phones to connect without interference from other mobile (cell) phones. [4 marks]

- Connections use (frequency/time/code) multiplex division to share frequencies
- Spread spectrum technology is used to allow multiple connections on same (set of) frequencies
- Multiple input and multiple output(MIMO) using multiple transmit/receive antenna to increase capacity/use of transmission channels/increased data flow
- Antennae from base stations/towers can be/are directional to avoid interference from other towers/reflections
- Adjacent cells use different frequencies from neighboring cells
- Connection/wireless frequencies are reused by cells distant from each other to increase capacity (where ranges of frequencies are limited)

Explain how 4G cellular networks provide a better service than 3G networks for smartphone users accessing internet services. [4 marks]

- Increased rate of data transfer/higher bandwidth

  - provides faster download/more buffering capacity/less waiting for data to download
  - Web pages/content loads faster
  - due to use of higher range of frequencies
  - due to use of Multiple input and multiple output (MIMO) using multiple transmit/receive antenna to increase capacity/use of transmission channels
  - connections use (frequency/time/code) multiplex division to share
  - due to use of spread spectrum technology to allow multiple connections on same (set of) frequencies
- Handovers between base stations are 'smoother'/less subject to interruptions/loss of connection
- Use (only) packet switching technology instead of circuit switching (as in 3G)
  - so IP packets can be carried/based on IP packet switched technology
- Packet switching allows data/voice packets to be multiplexed/interleaved with other packets (give increased rates of data flow)

Satellite Communication Systems

- A communication satellite is a machine that has been transported into space and set to orbit the earth.
- These satellites are used to transmit radio waves from one place to another
- The radio waves that are transmitted can carry telephones calls, internet data and television broadcasts
- The main components of a satellite are solar powered battery, a transponder and various antennas

How do they transfer and receive data for communication:

- Satellites remain in orbit over the earth so they appear stationary over desired areas.
- Multiple satellites could be arranged in constellation each providing coverage of small area of surface
- Satellites use spot beams to target specific area/user on earth

- Data intended to be sent is converted into radio waves and then transmitted from ground station to the satellite /space in the form of radio waves, this is called uplink
- The ground stations maintain permanent links with satellites at all time
- The satellite could be a chosen one or the nearest in orbit which picks up the radio waves as the recipient.
- They use antennas on satellite pick up and receive the radio waves
- The transponder processes the data, it also involves boosting signals to amplify it
- The antenna then transmits radio waves back to ground station on earth, this is called downlink
- The ground stations convert radio waves back to normal data and forwards it to the user

Global Positioning Systems (GPS)

- A GPS uses satellites to work out a user's current location through a process called triangulations/trilateration
- At least 2 low orbit satellites are required to map out the location
- Each navigation satellite constantly beams radio waves that are sent towards earth and picked up by ground stations/users device
- These signals contain data such as ID code of satellite, status information, current data and time and almanac data about where each GPS satellite is at any point in time
- The users device such as a mobile phone receives these radio signals/ or the nearest ground station
- A device must pick up these signals from 2 satellites for their 2d location to be pinpointed by the GPS, latitude and longitude
- 4 or more satellites allow 3d position to be calculate (i.e latitude, longitude and altitude), this is trilateration
- At most 3 are used to in triangulation process to find the location by using three lines of position
- The location is figured by calculating the intersecting points by timing signals from the satellite
- GPS is also used for surveillance purposes, by keeping a log of all GPS activity of a device
- A user can access that log and see where their device is or where they have been or where they currently at

14.12 Network security

Botnets

- It is a collection/group/number of internet-connected devices/smartphones
- (One or more) bot/malware is running on each/every (connected) device
- In it the security of (each/every) device has been taken over by third party
- It is controlled by third party/controller/bot herder via internet links
- Use of digital signatures to ensure that bot herder is only one available to direct/control bot/bot net
- Connection uses standard/usual internet protocol

Q: Explain how these botnets can be used to gain unauthorised access to data.

- The device has malware/bot installed without knowledge of user/owner
- These bots set up as clients on devices
- Bots can be setup as peer to peer with controller device aswell
- Bots connect together using internet communication protocols
- Bot controller/herder at remote location sends commands to bots using a device as a server/command and control
- Bots can automatically scan their computing environment to discover ways of propagating themselves to other devices
- Bot controller directs bots to gather keystrokes to discover login details
- Bots can execute/run other malware to access files/ gather data and send back to controller
- Botnets can carry out Denail of service (DoS) attacks on servers preventing legitimate use of files/data/services
- Botnets can send (spam/unwanted/fraudulent) disguised emails from infected devices with attached data/files/request for login credentials/financial details
- Botnets can distribute/direct spyware to gather use credentials/details/data and send to controller

- Botnets use computing resources without knowledge/permission of user and can compromise legitimate file/data storage

Malware

- User normally unknowingly downloads the malware (virus, spyware) onto their computer
- The malware is often disguised in a file download or a link that the user is enticed into clicking.

Third Party Attack:
Third parties may also want to hack computers to damage or steal data. Hackers will try to gain access to a system, normally by installing what is often known as a backdoor, in software. Third parties may also want to crack into computers to damage or steal data. Crackers will try a brute force approach to get into a computer by trying many different combinations of a password. They can also build software that will carry out this function for them. This allows them to gain unauthorized access to a computer system by using the user's log-in details.

data destruction: It is the deleting/removing of data, e.g. deleting a record from a database

data modification: It is changing data to a different value. The changed value is stored in the same location as the original, e.g changing value in cell of a spreadsheet from e.g. 100 to 101.

Describe ways that data can be protected from unauthorized destruction and modification.

- Security measures to detect/prevent unauthorised access to network/network connections
- Segmenting/zoning network sections/servers to prevent/reduce access by intruders
- Use of firewalls to prevent unauthorised access/intrusion to networks/network storage
- Use of VPN/secure connections to cloud storage systems
- Use of authorisation/authentication techniques for gaining access to data
- Regular/automatic check on data integrity with automatic alters/alarms/notifications (if data change is not authorised)
- Use of (high-level/256-bit) encryption techniques to restrict access/understanding or data so amendment of data is more difficult

Individuals and organizations can put a range of preventative methods in place to help protect their data.

- The simplest form of protecting data is the use of physical methods. Organizations can put a barrier to entry at the opening of their office or building.
- Other physical methods that could be used are CCTV, security guard and alarm systems. CCTV will allow an organization to see who is trying to gain unauthorized access.
- Places of this nature could also be secured using an alarm system, this will alert the organization if unauthorized access is attempted.

Data can also be protected using software-based methods.

- An employee may be required to provide biometric data, such as their fingerprint, iris, or facial features, to access data. Biometric devices are useful because biological data is unique to the user and very difficult to fake.
- The effects of malware can be prevented by using software, such as anti-malware, anti-virus, and anti-spyware software.
- This type of software is designed to scan a computer system for malware. If it finds any, it quarantines the malware (put it in a designated safe area) and allows the user to delete it.
- A firewall is another method that can be used to prevent unauthorized access or damage to data. A firewall can be hardware based or software based. A firewall examines incoming and outgoing traffic to a computer or a network. The firewall can be set to recognize malicious traffic by providing it with rules and criteria to check the traffic.

One way that an organization can protect data is to only allow access to those that directly need that data. This is called access rights. The username that an employee is given in an organization is often what indicates their access rights.

One final method that an organization and an individual can use to protect their data is encryption. Encryption will not stop the data from being stolen, but it will mean that if the data is stolen, it will be meaningless to the third party, unless they are able to get the key to decrypt it.

The Impact of Security threats on individuals and organizations

Individuals and organizations need to carefully consider the impact of security threats. There are two main common reasons why perpetrators carry out security attacks –either to obtain personal data or as an act of sabotage or revenge.

Individuals need to be very cautious of any of their personal data being accessed and stolen. This could lead to criminal acts such as **fraud and theft of their identity**. Organizations need to be very cautious of any of their stored data being accessed and stolen. They also need to be very cautious of their data being manipulated or destroyed. Data is a very precious asset to organizations, as it is used in the day-to-day functioning of the organization. Without it, they are unlikely to be able to function at all. This could lead to a loss of profits, or if the data is stolen because the organization's security is breached, this could lead to a negative reputation for the organization, which may also lead to **a loss of profits.**

Q: Data that is transmitted on networks or stored on servers needs to be protected. Analyse the use of software methods to protect data.

Question	Answer	Marks
9	***Analyse: examine in detail to show meaning, identify elements and the relationship between them.*** ***Seven from e.g.:*** • Use of regularly updated/up-to-date anti-malware/anti-virus/anti-spyware software to protect against malware … • … provides real-time monitoring/alerts to continually protect data/isolate/delete/remove infections/compromised files/data • Use of encryption to make data unintelligible/not understood by unauthorised users/viewers … • … prevents theft/misuse of personal/financial/confidential information • Encryption of hard disks/USB devices/removable storage so that if lost the content of data is unusable/inaccessible … • … requires user to remember the password else data is lost • Biometrics used to compare existing/stored unique ID data with newly presented ID data for authentication of user ID … • … allowing access only to authorised users to areas/devices/laptops/tablets/smartphones storing data • Use of access rights/permissions on files/folders to control user access with Access Control Lists/ACLs … • … which have allow/deny entries • Use of passwords on individual files … • … to control user access • … encrypt documents • … control editing rights to prevent unauthorised viewing/reading/alteration of content • Use of steganography/hide data within other data/text in JPEG images/MP3 files requiring the use of secret key/public/private key encryption … • … that unauthorised users are unaware of the data/cannot access the information in the data • Use of automatic backup schedules to ensure that (copies of) data is regularly stored elsewhere … • … can restored/retrieved if original lost/damaged. • Use of regular software updates/updates to applications/apps … • … ensure that security issues are addressed/corrected as soon as possible. ***Max 5 marks if bullets/list of points/characteristics.***	7

14.13 Disaster recovery management

Disaster recovery is a planning mechanism that allows an organization to plan for disaster and put in place measures that will minimize the risks. To be able to plan for protection against a disaster, the possible disaster first needs to be identified. There are several stages that could be used to identify a risk that could cause a disaster, these include:

Stage	Description
Risk Analysis	This is also known as a risk assessment, they will carry out qualitative risk analysis to prioritize risks for analysis and quantitative risk analysis for the likelihood of occurrence and their consequences. The organization will first identify what they think could be a potential disaster. They will then consider what or who could be harmed as a result. They will finally think about how this could impact the organization, such as loss of access to premises, loss of data and skills and loss of its function.. Finally, they will develop methods to control the possibility and impact of the disaster. They will produce a report of the risks. They will produce a computer simulation of the disaster. All parts of a company that could cause disaster in an organization may be a power cut, cyber-attack, fire, flood, denial of access to data, theft of data, corruption of data and hardware failure
Perpetrator Analysis	This process is often carried out as part of the risk analysis. The organization will identify who they think could be a perpetrator that could cause a disaster to occur. A perpetrator is someone who carries out malicious or illegal acts
Risk Testing	In this stage of the process an organization will rehearse the plans and strategies that have been developed during the risk analysis. This will allow employee in the organization to understand exactly what they should do in the event of disaster. An organization can monitor what happens during the testing stage and can amend plans to take improved actions or to correct the behavior of employees, if they are not acting correctly, the type of plans and strategies that could be tested are: • Restoration of data • Replacement of hardware • Reinstallation of software • Emergency evacuation of offices • Emergency protection methods of data
Quantifying the Risk	The process of quantifying a risk involves evaluating the risk and prevention method for the risk in terms of cost and time There are two key measurements that should be considered, maximum tolerable downtime (MTD) and recover time objective (RTO)

	• MTD is the maximum time that each part of the organization could tolerate not having access to the essential parts of a network that they require. • RTO is the estimated maximum amount of time in which an organization has in which to recover its network and resume operations.

How to detect threats and prevent disaster

- Power surge protection devices could be used to stop a surge in power damaging hardware
- A backup generator could be ready for use if an organization suffers power failure
- Backups of data could be stored in fire and flood proof cases so that data isn't lost in a fire or flood.
- Policies and procedures should be developed for staff to follow to prevent disaster such as fire and damage to equipment
- Cloud computing could be used as a backup for data and possible hardware resources
- Backups made and sent off site at regular intervals
- Backups made on site and automatically copied to offsite disk
- Backups made directly to offsite/remote/'cloud' servers
- Local mirrors of systems and/or data and use of disk protection technology such as RAID
- Use of fire extinguishers/mitigation systems such as alarms and fire extinguishers
- Use of antivirus software to protect data against corruption/loss/deletion
- Use of firewalls to prevent unauthorized/control access
- Use of physical security measures to control access by personnel
- Important passwords/codes should be held by more than one person/in secure conditions but accessible in an emergency

How to restore after a disaster

- Activate the disaster recovery plan
- Access and assess the damage and recover based on criticality
- The restoration of data from backups
- The re installation of software
- Replacement or repair of hardware